

Curs 4

Struct. algebrice în informatică

Elemente speciale într-o mulțime ordonată

Fie (M, \leq) o mulțime ordonată

Def: Elementul $x \in M$ este MINIM (sau prim element) dacă și $y \in M$: $x \leq y$

Def: $-/-$ este MAXIMAL (sau ultim element) dacă și $y \in M$, $y \leq x$

Def: $x \in M$ este ELEMENT MINIMAL dacă și $y \in M$, $y \leq x \Rightarrow y = x$ (nu găsim elem. struct mai mici decât x) (în M)

Def $x \in M$ este element MAXIMAL dacă și $y \in M$, $x \leq y \Rightarrow x = y$

Proprietăți: dacă $x \in M$ este minim sau maxim, atunci este unic.

• În plus, x este singular element minimal, respectiv maximal din (M, \leq)

Def: Pp că x_1, x_2 sunt proprietate de minim în M

x_1 -minimum $\Rightarrow x_1 \leq x_2 \wedge x_1 = x_2$, deci minimul (dacă) este unic

x_2 -minimum $\Rightarrow x_2 \leq x_1$

Analog pentru maxim!

Fie $z \in (M, \leq)$ - un el. minimal | def $\rightarrow x = z$, dec.
cum x -minim $\rightarrow x \notin z$
 x este unicel
element minim
pe (M, \leq)

Exemplu:

(\mathbb{N}, \leq) - 0 este minim și singurul elem.
minimal

\emptyset maxim, \emptyset el. maximal

(\mathbb{Z}, \leq) - \emptyset minimal, \emptyset maximal, \emptyset
minim, \emptyset maxim

demo lui Zorn

Fie (M, \leq) - multime ordonata cu prop.

că + submultime o se total
ordonat (= lini) are un majorant.
Atunci \exists elem. maxim elem. maximal

în (M, \leq)

Def: (M, \leq) s.m. multime bină ordonată -
dacă orică revedea submultime
un prim element.

ex: (\mathbb{N}, \leq)

obs! dacă (M, \leq) este bină ordonată $\Rightarrow (M, \leq)$ este
total ordonat

XIII

Fie $x, y \in M$, atunci $\{x, y\}$ are un minim.
 Dacă x este minimul $\Rightarrow x \leq y$, iar dacă y
 este maximul $\Rightarrow y \geq x$

Teorema lui Zermelo

Pentru orice multime nevidată M , putem defini o relație
 de ordin \leq a.î. (M, \leq) să fie bineordonat.

Axioma alegorii \Leftrightarrow Lemă lui Zermeloa

Aritmetică în \mathbb{Z}

Def: Fie $a, b \in \mathbb{Z}$. Spunem că $a|b$ dacă $\exists k \in \mathbb{Z}$.

$a|b \Leftrightarrow a \cdot k = b$
 Spunem că b se divide cu a , NOT $b : a$

" $|$ " o relație pe \mathbb{Z}

a) reflexivă: $\forall a \in \mathbb{Z}$, $a = 1 \cdot a$ dică $a|a$

b) transițivă: $\forall a, b, c \in \mathbb{Z}$, $a|b$ și $b|c \Rightarrow a|c$

$$\Rightarrow \begin{cases} b = a \cdot k_1, & k_1 \in \mathbb{Z} \\ c = b \cdot k_2, & k_2 \in \mathbb{Z} \end{cases} \Rightarrow c = a(k_1 \cdot k_2) \Rightarrow a|c$$

Def Spunem că $a, b \in \mathbb{Z}$ sunt asociate în divizi-
 bilitate ($a \sim b$) dacă $a|b$ și $b|a$.

Obs! dacă $a, b \in \mathbb{Z}$ cu $a \sim b \Rightarrow a/b \neq b/a$

$$\Rightarrow b = a \cdot k_1 \quad \text{și} \quad \text{dacă } k_1, k_2 \in \mathbb{Z} \Rightarrow b = b(k_1 \cdot k_2)$$
$$a = b \cdot k_2$$

$$\Rightarrow \text{dacă } b \neq 0 \Rightarrow k_1 \cdot k_2 = 1 \Rightarrow k_1 = k_2 \in \{-1, 1\} \Rightarrow$$
$$\Rightarrow b = \pm a$$

$$\text{dacă } b = 0 \Rightarrow a = b \cdot k_2 = 0 \Rightarrow b = 0$$

dacă $a \in \mathbb{Z}$, $a \sim b \Leftrightarrow a = \pm b \Leftrightarrow |a| = |b|$

dacă „ \sim ” pe \mathbb{Z} este antisimetrică: $a \sim b \wedge b \sim a \Rightarrow a = b$

Prop⁺ (\mathbb{N}, \sim) este multime ordonată

1 este cel mai mic element (minimum)

0 este cel mai mare element (maximum)

$\forall a \in \mathbb{Z}$

$|a|/a$

$a/0$

$a \cdot 0 = 0$

$a/0 \in \mathbb{N}^*$ și $a/0 = 0, a \leq 0$

dacă $a, b \in \mathbb{N}^*$ și $a/b = 0, a \leq b$

Prop: dacă a/b_1 și a/b_2 în \mathbb{Z} , atunci

Prop⁺: dacă a/b_1 și a/b_2 în \mathbb{Z}

$a/(u \cdot b_1 + v \cdot b_2)$, $\forall u, v \in \mathbb{Z}$

dacă $a/b_1 \Rightarrow b_1 = a \cdot k_1, k_1 \in \mathbb{Z}$

$a/b_2 \Rightarrow b_2 = a \cdot k_2, k_2 \in \mathbb{Z}$

$\Rightarrow u \cdot b_1 + v \cdot b_2 = a(\underbrace{u \cdot k_1 + v \cdot k_2}_{\in \mathbb{Z}})$, deci $a/(u \cdot b_1 + v \cdot b_2)$

Teorema de împărțire cu rest

Pentru $a, b \in \mathbb{Z}$, $b \neq 0$ există numere

$q, r \in \mathbb{Z}$, $a = b \cdot q + r$ și $0 \leq r \leq |b|$

q = cotaul împărțirii lui a la b
 r = restul împărțirii lui a la b

DIM: $r = \min \{ a - b \cdot x \mid x \in \mathbb{Z} \text{ și } a - b \cdot x \geq 0 \}$

pt acest r , $\exists q \in \mathbb{Z}$ cu $r = a - bq$

Să se arate că $\{r\} \neq \emptyset$

$a \geq 0 \Rightarrow$ pt $x=0$ avem $a - b \cdot 0 = a \geq 0$

$a < 0 \Rightarrow \dots$

Deci $\exists r$ cu $r \geq b$

\Rightarrow deci $b \geq 0 : 0 \leq r - b = a - b(q+1)$,
contradicție minimalitatea lui r .

\Rightarrow deci $b < 0 : 0 \leq r + b = a - b(q-1), \dots$

Deci $0 \leq r < |b|$

Unicitatea: $\text{Pp. că } a = b \cdot q + r = b \cdot q_1 + r_1, q_1, r_1 \in \mathbb{Z}$

$$0 \leq r_1 < |b|$$

$$b(q-q_1) = r_1 - r$$

$$|b||q-q_1| = |r_1 - r| \leq |b|$$

$$\Rightarrow |q-q_1| = 0 \Rightarrow q = q_1 \Rightarrow r = r_1$$

$$0 \leq r_1 < |b|$$

$$\Rightarrow 0 \leq (r-r_1) < |b|$$

El mai mare div comun (c.m.m.d.c)
El mai mic multiplu comun (c.m.m.m.c)

g.c.d (greatest common divisor)

lcm (least common multiple)

Def Spunem că lez este lcm-ul lor dacă:

(1) este divizibil

(2) (a) lez și alți divizibili \Rightarrow $d \mid l$

Def Spunem că d este gcd-ul lor dacă:

(1) $d \mid a$ și $d \mid b$

(2) și d, că cu $d_1 \mid a$ și $d_1 \mid b \Rightarrow d_1 \mid d$

Teorema $\forall a, b \in \mathbb{Z}$, $\text{gcd}(a, b)$, $\text{lcm}(a, b)$ există și sunt unice până la asociere în divizibilitate.

$$\text{lcm}(a, b) = \frac{a \cdot b}{\text{gcd}(a, b)}$$

Def $d_1 \sim d_2 \Leftrightarrow d_1 \mid d_2$

Prop În \mathbb{Z} : $d_1 \sim d_2 \Leftrightarrow d_1 \mid d_2 \wedge d_2 \mid d_1 \Leftrightarrow d_1 = \pm d_2$
poisă $d_1 \neq d_2$ au proprii divizori comuni \Rightarrow însăși $d_1 \mid d_2 \wedge d_2 \mid d_1 \Leftrightarrow d_1 = \pm d_2$

Def $d_1 \mid d_2 \wedge d_2 \mid d_1 \Leftrightarrow d_1 = \pm d_2$
 $\text{gcd}(a, b)$ și poach calcul de Alg. lui Euclid,

input: $a, b \in \mathbb{Z}$

output: $d = \text{gcd}(a, b) \wedge u, v \in \mathbb{Z} \wedge a \cdot u + b \cdot v = d$

Prop $b = 0$, atunci $d = a$
 $a = 1 \cdot a + 0 \cdot b$
 $0 < r_1 < |b|$

$b \neq 0$, atunci $a = b \cdot q_1 + r_1$ cu $0 < r_1 < |b|$
 $b = r_1 \cdot q_2 + r_2$
 $r_1 = r_2 \cdot q_3 + r_3$